



OAC Boletín de Abril de 2019

"No comprender la importancia futura de los guerreros del ciberespacio (técnicos, especialistas, neurocientíficos, psiquiatras, psicólogos, pero por sobre todo estrategas), condenará a las fuerzas militares, que no se preparen para la guerra en las mentes de la sociedad. Lo que la infantería fue a Napoleón ("Reina de las Batallas") en el futuro serán los ciberguerreros a la conciencia del conflicto ("reyes de la guerra")

Alejandro Moresi
Observatorio Argentino del Ciberespacio

Contenidos

CIBERDEFENSA.....	2
Las relaciones cívico – militares ante los ataques cibernéticos	2
Redes sociales, el ambiente para experimentar la guerra por las mentes	2
Rusia emplea interferencias de GPS en la protección de autoridades	2
CIBERGUERRA.....	3
La 'cibertrinchera' de Occidente	3
En la era de la guerra electrónica ¿debemos volver al empleo de las palomas?.....	3
Francia reconoce que empleará operaciones cibernéticas ofensivas.....	3
CIBERSEGURIDAD	3
¿Cómo pensar por sí mismo frente a las "fake news"?	3
La Ciberseguridad en las estructuras crítica interrelacionadas.....	3
Documento de Interés.....	4
Informe anual de Seguridad	4
CIBERCONFIANZA	4
Los datos de Facebook, continúan siendo con problemas de seguridad.....	4
CIBERFORENSIA	4
Desbloqueo, cifrado y administración de claves para almacenamiento de datos militares.....	4



El Observatorio Argentino del Ciberespacio (OAC), micro-sitio de la Escuela Superior de Guerra Conjunta

URL: <http://www.esgcffaa.edu.ar/esp/oac-boletines.php>.

Esta publicación es posible gracias al financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en la **Antena Territorial de Defensa y Seguridad**, que administra el **Centro Tecnológico y Perspectiva Mosconi** de la Facultad de Ingeniería del Ejército Argentino

Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

CIBERDEFENSA

Las relaciones cívico – militares ante los ataques cibernéticos

En tiempos de persistentes ciberataques ¿es posible diseñar una estrategia de ciberseguridad entre las autoridades civiles y las militares que al mismo tiempo que busque proteger a un país de los ataques cibernéticos no ponga en peligro las libertades civiles y el libre flujo de información?, de esto nos hablan Benjamin Jensen and J.D. Work

<https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/>

Redes sociales, el ambiente para experimentar la guerra por las mentes

El marketing parece una cuestión frívola, pero es un campo de experimentación constante basado en datos, en la última década los sitios de redes sociales como Facebook se han convertido en laboratorios de vanguardia para perfeccionar los mensajes de influencia. En el mercado de la revolución de la información, la organización con la mayor cantidad de datos y la capacidad de utilizarla gana.

https://www.afcea.org/content/welcome-social-cyber-warfare?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email#

Rusia emplea interferencias de GPS en la protección de autoridades

Un grupo de expertos de los EE.UU., han notado que ocurre algo extraño cuando el presidente ruso, Vladimir Putin, se acerca a un puerto: el GPS, el fenómeno sugiere que Putin viaja con un dispositivo de suplantación de GPS móvil, aparentemente se estarían manipulando los sistemas de navegación global en una escala mucho mayor de lo que se entendía anteriormente.

<https://foreignpolicy.com/2019/04/03/russia-is-tricking-gps-to-protect-putin/>



CIBERGUERRA

La 'cibertrinchera' de Occidente

Así se titula la nota de Belén Domínguez Cebrián para el diario El País de España donde comenta que en Tallín (Estonia) se trabaja sobre un escenario como este: “Las centrales eléctricas de un país occidental se colapsan, los clientes de los bancos no pueden acceder a sus cuentas corrientes, el tráfico civil por tierra, mar y aire es un caos porque los mandos de control se han caído, y el agua que sale de los grifos está contaminada con agentes químicos. Los medios de comunicación son incapaces de explicar qué sucede. Y la gente está en peligro, desconfía del sistema. Esto es un “ciberataque”.

https://elpais.com/internacional/2019/03/04/actualidad/1551720675_282520.html

En la era de la guerra electrónica ¿debemos volver al empleo de las palomas?

Frank Blazich nos acerca un análisis de lo que algunos autores denominan “guerras híbridas” y otros “nuevos tipos de guerra”, ellos han demostrado que el empleo de nuevos métodos y medios de combate están limitados solamente por la iniciativa y la imaginación. No sería de extrañar que en el caso que se interrumpen o desactiven las comunicaciones militares, las palomas vuelvan a prestar servicio en las fuerzas armadas como ya lo hacen en China y Francia.

<https://warontherocks.com/2019/01/in-the-era-of-electronic-warfare-bring-back-pigeons/>

Francia reconoce que empleará operaciones cibernéticas ofensivas.

Nicole Lindsey Si bien algunos países como el Reino Unido aún mantienen una política defensiva, otros como los Estados Unidos de América en 2018 y ahora por Francia han decidido adoptar el empleo de operaciones ofensivas en el ciberespacio.

<https://www.cpomagazine.com/cyber-security/france-latest-nation-to-acknowledge-offensive-cyber-operations/>

CIBERSEGURIDAD

¿Cómo pensar por sí mismo frente a las “fake news”?

David S. Maxwell, escribe acerca de cómo la sociedad debe empezar a tomar conciencia de todo lo que arrastran consigo las noticias falsas “fake news”, que son difundidas a través de portales de noticias y sobre todo las redes sociales, que buscan básicamente desinformar o incluso llevar a engaño a los ciudadanos.

<https://smallwarsjournal.com/jrnl/art/the-cyber-underground-%E2%80%93-resistance-to-active-measures-and-propaganda-%E2%80%93-the-disruptors%E2%80%93mot-0>

La Ciberseguridad en las estructuras crítica interrelacionadas

Robert K. Ackerman, nos advierte acerca de la creciente interconexión entre los elementos de las infraestructuras críticas, su salvaguarda contra amenazas físicas y cibernéticas debe ser cada vez más sofisticado, debido a que muchos elementos de la infraestructura crítica dependen unos de otros, y asegurarlos es un esfuerzo coordinado, es un desafío constante.



https://www.afcea.org/content/critical-infrastructure-protection-looks-inward?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email#

Documento de Interés

Informe anual de Seguridad

Se presenta el informe anual de seguridad español, entre las páginas 61 y 73, presenta un interesante informe acerca de la situación de Ciberseguridad española y varios datos de nivel internacional.

<https://www.dsn.gob.es/sites/dsn/files/IASN2018.pdf>

CIBERCONFIANZA

Los datos de Facebook, continúan siendo con problemas de seguridad

Investigadores de la compañía UpGuard descubrieron dos datasets distintos: la primera pertenece a una compañía de medios mejicana llamada Cultura Colectiva y la otra a una app integrada en Facebook llamada At the pool. Los datos recolectados por Cultura Colectiva contienen 540 millones de registros de usuarios. Incluyen: comentarios, likes, nombres de cuenta, ID de usuario de Facebook, entre otros datos.

<https://thehackernews.com/2019/04/facebook-app-database.html>

CIBERFORENSIA

Desbloqueo, cifrado y administración de claves para almacenamiento de datos militares

Mercury System ofrece un documento (white paper) en la idea de que las armas y los guardias solo pueden usarse para proteger datos de alto valor, pero solo es cuestión de tiempo antes de que un enemigo suficientemente capacitado encuentre una forma de evitar estas defensas físicas, se deben implementar estrategias bajo el supuesto que el dispositivo puede caer en manos del enemigo haciendo impracticables el uso de los datos. El documento puede ser obtenido en

<https://info.mrcy.com/1811-WP-MSS->

[UnlockingtheTrueValueofEncryptionandKeyManagement_ShortformLP.html?ch=SignalCyberEdge2.19](https://info.mrcy.com/1811-WP-MSS-UnlockingtheTrueValueofEncryptionandKeyManagement_ShortformLP.html?ch=SignalCyberEdge2.19)

*Copyright © */2018|* */Escuela Superior de Guerra Conjunta|*, All rights reserved.*

/Observatorio Argentino del Ciberespacio |

Nuestra dirección postal es:

/Luis María Campos 480 - CABA - República Argentina |

Nuestro correo electrónico:

/observatorioargentinodelciberespacio@conjunta.undef.edu.ar |

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe from this list](#).